COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

500 WEST TEMPLE STREET
493 HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

TELEPHONE: (213) 974-2008
FACSIMILE: (213) 633-4733

August 14, 2003

To: Supervisor Yvonne Brathwaite Burke, Chair
Supervisor Don Knabe, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider
Chief Information Officer

Subject: **MICROSOFT COMPUTER WORM – W32.BLASTER.WORM**

The Microsoft Computer Worm, W32/Blaster.Worm, also referred to as W32/Lovsan infected multiple County computers on Monday, August 11, 2003. The worm was detected and our response began about 1:30 p.m. The departments that were most significantly affected were the Assessor's Office and the Department of Health Services; however, other departments were affected as well.

Microsoft issued a security bulletin on July 16, 2003 announcing the vulnerability in their systems along with code (security patch) that was designed to fix the problem. This notice was subsequently published by the County Computer Emergency Response Team (CCERT) to the various department CCERT members recommending that systems be updated.

The Microsoft patch needed to be installed in desktop computers as well as servers that use most of the active Microsoft operating systems. The W32/Blaster worm that exploited this vulnerability infected approximately 1,000 desktop devices as well as a few servers that had not been updated with the security patch. This is out of the approximately 53,000 computing devices within the County. The departments that were not infected either had older operating systems or had properly deployed the Microsoft security patch that was designed to protect against this type of worm.

As part of a coordinated response, ISD's Data Security took action to prevent the entry of the W32/Blaster worm by blocking this code from entering the County networks at the Internet connection. Preliminary investigation has disclosed that the worm actually entered the County network through a point other than the ISD Internet connection. Once inside the County network, it quickly spread across multiple departments infecting their machines. The source of the worm's entry is under more thorough investigation.

The anti-virus companies that supply County antivirus software began releasing updates to address the W32/Blaster worm on August 11, 2003, once the worm was discovered. The updates would discover the worm in infected machines. Later in the day, the updates were able to delete and quarantine the worm.

In the past year, the County's security initiative led by my office implemented an Intrusion detection system (IDS) that can also block specific types of malicious network traffic. This system was first employed to contain the Slammer Worm and proved itself effective during this worm attack. The detection code that was installed specifically for the W32/Blaster worm is effective against any variants of worms that exploit this Microsoft vulnerability. Those worms (not yet seen here) include W32.RPCSDBOT.A, W32.Blaster-A and Win32.Posa.

The intrusion detection system that has been deployed across the County was able to discover the attack as well as specifically pinpoint and disable infected machines. The ISD Helpdesk and Information Security organizations were able to notify departmental technical staffs to repair the infected machines. While the worm is effectively contained, the system continues to detect a few infected machines and direct corrective actions.

Upon discovery of the County infections, the Chief Information Security Officer activated the CCERT coordination efforts and initiated a countywide series of conference calls to status user problems and announced required actions for the departments. These meetings continued until it was determined that the worm was contained on August 14, 2003. Follow up meetings will be initiated to assess the impact of this infection as well as document lessons learned and improvements that should be implemented in the County's overall response effort.

JWF:AB:jsl

c: Executive Officer, Board of Supervisors
Chief Administrative Officer
County Counsel
Chair, Information Systems Commission